**ФЕДЕРАЛЬНОЕ АГЕНСТВО СВЯЗИ  
Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. Проф. М. А. Бонч-Бруевича»  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Кафедра Защищенных систем связи  
Дисциплина «Основы криптографии»  
  
  
  
**Лабораторная работа №** **6  
  
  
Изучение и исследование блокового шифра AES**

**Вариант 4**Выполнил: ст. группы ИКТЗ-83  Громов А.А.

Проверил: Профессор кафедры ЗСС: д.т.н. проф. Яковлев В.А.

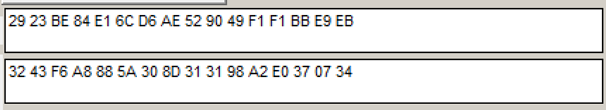
**Цель работы**

Изучить преобразования, выполняемые при шифровании и дешифровании сообщений в блоковом шифре AES, а также исследовать некоторые его свойства.

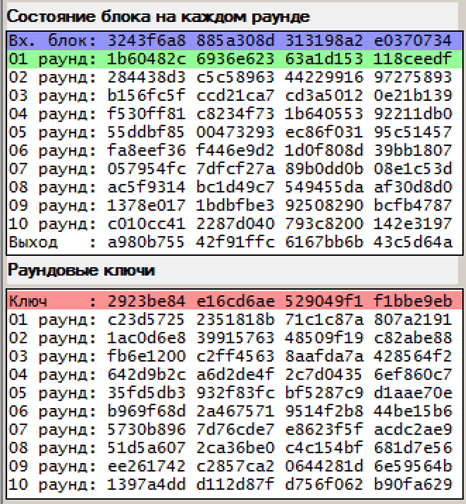
# Используемое программное обеспечение

Для выполнения работы используется специальная программа “AES.exe”

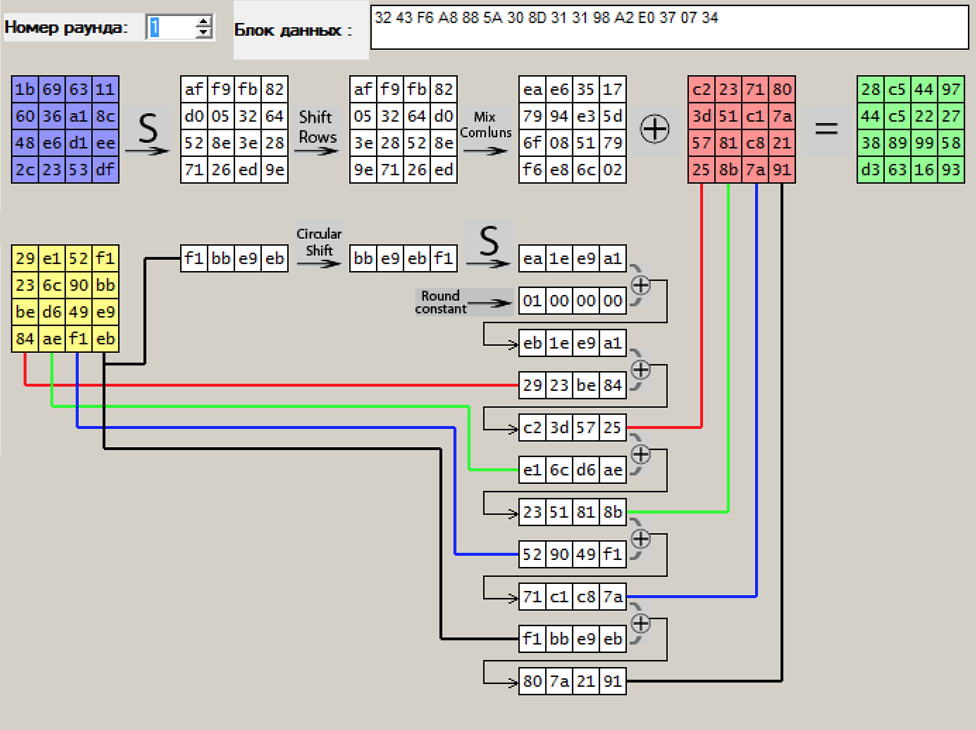
1. Случайно сгенерированные ключи и блоки данных.

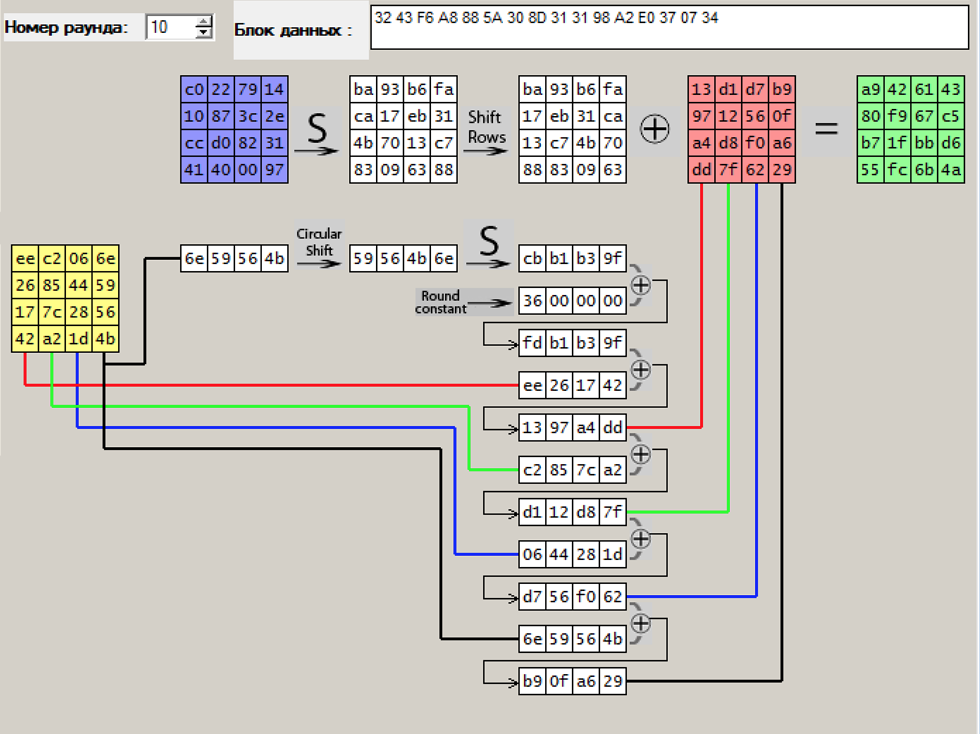
****

1. Шифрование данных
   1. Состояние блоков и раундовые ключи

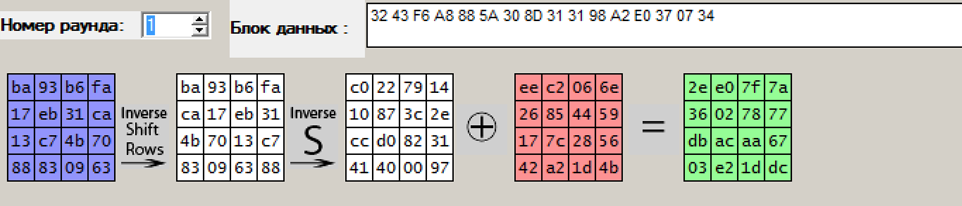


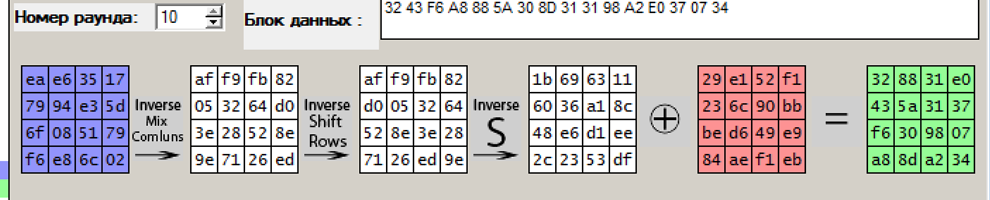
* 1. Примеры раундов шифрования(1,10)





1. Расшифрованиеданных
   1. Примеры раундов расшифрования(1,10)





1. Преобразование S - 1ый раунд (Вариант 4)

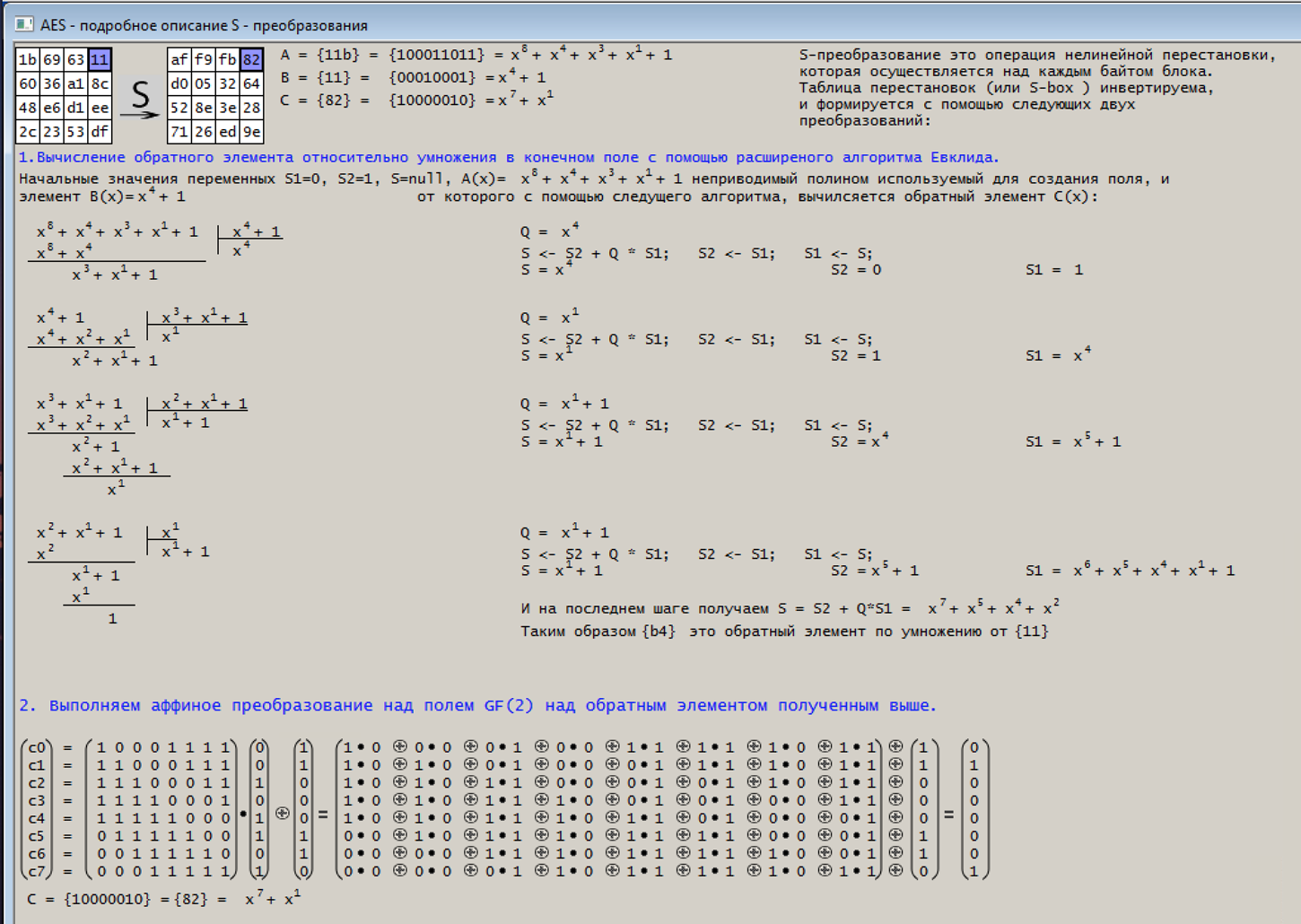
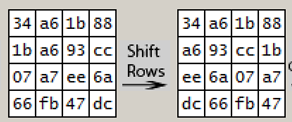


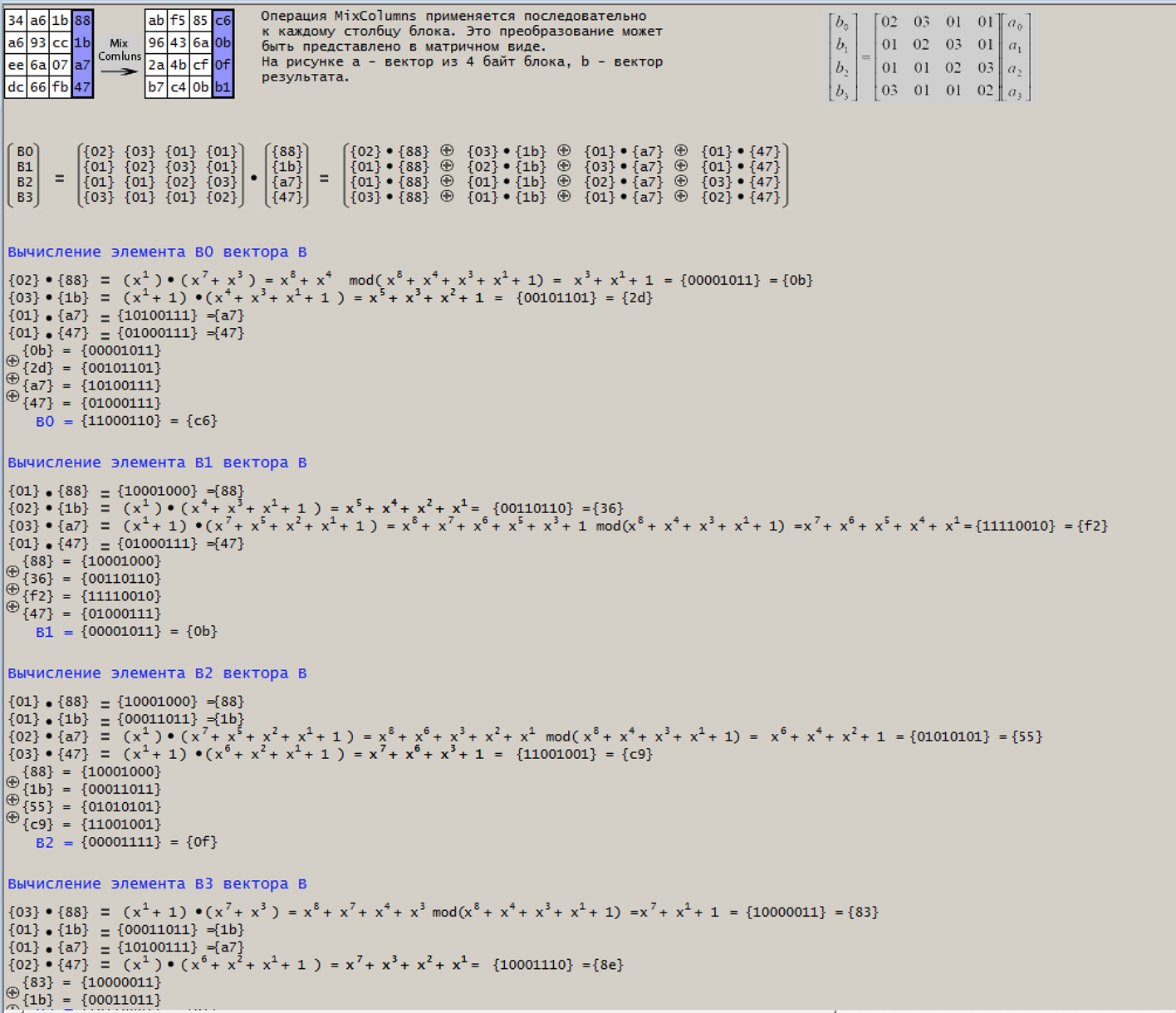
фото с бумажки

В остатке получилась 1, следовательно, обратный элемент вычислен правильно.

1. Shift Rows:



1. Mix Columns – 1-ый раунд (Варивнт 4)

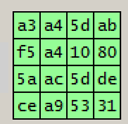


1. Нулевой ключ:



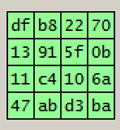
1-ый раунд:





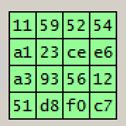
2-ой раунд:





3-ий раунд:

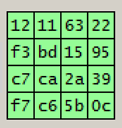




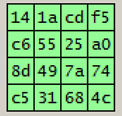
1. Нулевой блок:



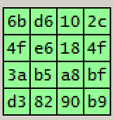
1-ый раунд:



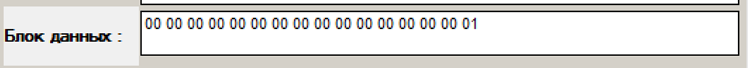
2-ой раунд:



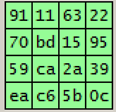
3-ий раунд:



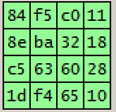
1. Сообщение с одной единицей:



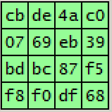
1-ый раунд:



2-ой раунд:



3-ий раунд:



**Вывод:**

В ходе выполнения данной лабораторной работы мы изучили преобразования, выполняемые при шифровании и дешифровании сообщений в блоковом шифре AES, а также исследовали некоторые его свойства. По результатам из п. 7-9 можно сделать вывод, что число изменившихся бит после каждого преобразования (SubBytes; ShiftRows; MixColumns и AddRoundKey), с повышением номера раунда, увеличивается.